ANALYSIS OF INTERNET OF THINGS ECOSYSTEM EFFECTIVENESS BASED ON OBJECT CAPABILITIES WITH DEEP LEARNING ALGORITHMS

A SYNOPSIS

Submitted by

SENTHIL KUMARAN. S
(Reg. No. 201412216)

in partial fulfillment for the award of the degree of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(DEEMED TO BE UNIVERSITY)

ANAND NAGAR, KRISHNANKOIL – 626 126

TAMIL NADU, INDIA

APRIL 2023

1. INTRODUCTION

Internet of Things or IoT is a global network connecting machines, infrastructures and environments, which have started spreading like a wild fire touching every single aspect of our lives within two decades of its birth from ARPANET. This new creative era of embedded technology is pervasive and amazingly has the potential to offer boundless opportunities in augmenting our lives through its innovations and applications with each passing day. From smart phones to smart cities, expectations have grown from simple devices to intelligent embedded smart machines. To accomplish the above dream of intelligent digital world, IoT paradigm integrates data collection, exchange of communication, machine learning, AI, Big Data, cloud environments to create a smart and efficient Internet of Everything. Different participating technologies of IoT are illustrated in Figure 1.

There are many critical reasons for this rapid explosion of IoT growth:

- Pervasively available internet connectivity
- Lowering costs of devices and sensors
- Considerable increase in Computer power
- Increased use of Smart phones and computers
- Less storage and data collection issues due to cloud based solutions

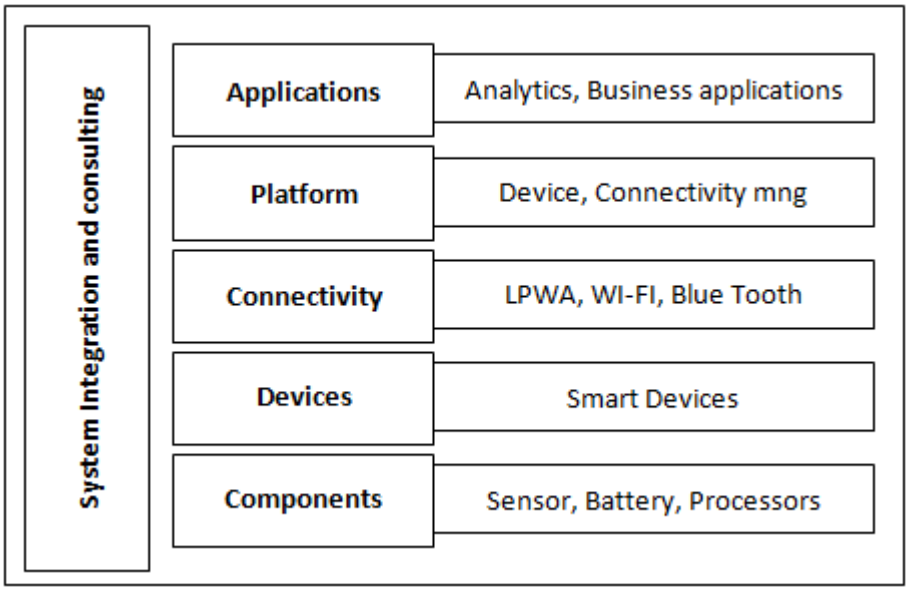

Figure 1: IoT Technology

To understand the basic working of IoT ecosystem, it becomes essential to know its components which are illustrated in Figure 2. IoT is not a single isolated technology, it's a mix of enabling technologies that enables IoT to acquire, process, authenticate and enhance the security and efficiency of the information obtained. The main distinction between internet and IoT lies in imbibing intelligence as a functional requirement for the operation of IoT devices. Hence IoT is a congregation of hardware and software techniques to collect, store, analyze and communicate among multiple devices and environments [1].

IoT has given a new dimension to human lives by connecting them with smarter devices and access them anytime, anywhere, any place to deliver value added services and perform distinguished tasks. IoT middle-ware platforms with their ready to use features enable cross device interoperability, compatibility, uncomplicated automation, management and provisioning of devices within an IoT ecosystem. Potential areas where IoT is applied is diverse and numerous as they permeate into every single aspect of humans, right from society to industries, smart homes to institutions, hence their applications envelop heterogeneous areas such as agriculture, smart cities, medicine, industrial automation etc.,

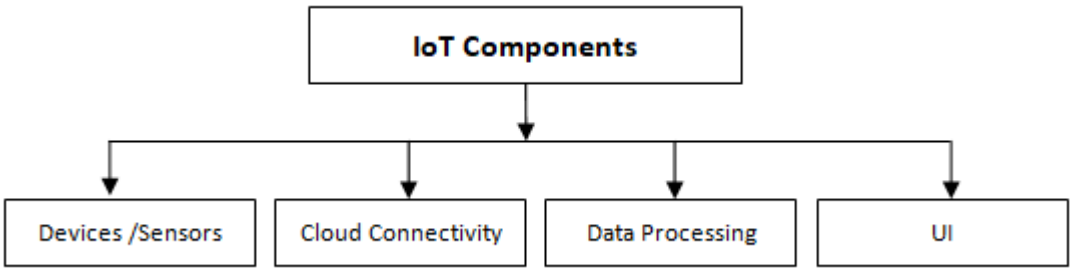

Figure 2: IoT Ecosystem Components

The following are the important and specific challenges [2] that should be addressed and resolved by designers, developers, researchers and manufacturers to attain the desired outcome and ensure the successful functioning of the IoT system.

- Data management
- Continuity
- Compliance
- Monitoring
- Security and Privacy
- Communication

- Interoperability
- Coexistence

2. LITERATURE REVIEW

Fengwei et al. [3] reviews the strategies taken by multiple nations to adopt this framework. Few countries like Japan are taking a bottom up approach and few other countries in Europe takes a top down approach towards IoT and Industry-4.0. Interesting finding from this article is US started adopting this in 2011 even before this standard was formally publicized.

Anichur Rahman et al. [4] discuss multiple ways to access sensor information in multi-hop network. Wearable devices use variety of sensors to collect critical information that helps in health care and diagnosis of patients - Yeung et al. [5]. This study presents detailed review of sweat sensors used in wearable devices. Author also presents the challenges and gaps in developing applications based on sweat sensors.

Brizzi et al. [6] created a prototype to remotely control a robot and to sense amount of energy consumed and gallons of water used in an industrial environment. This information is collected in real time using IoT sensors, where every module in production environment is controlled remotely. Author in his prototype uses EBBITS middle-ware that exposes the information collected as a web service to the external world.

Babun et al. [7] in their research describes a high-level evaluation framework which uses variety of criteria to compare and analyze IoT platforms used across multiple domains. Existing comparison methods available in the market are based on 1) Functionality of IoT device and the domain where it is used, 2) Cost of implementation, 3) On demand expansion, 4) Security. But all IoT platforms are distinct and they are created for different use cases. Comparing them directly is not going to give effective results. Author has proposed a novel way to compare the IoT platforms, which uses the below attributes:

- Design and Topology considerations
- Support for programming languages
- Integration with 3rd party apps
- Support for multiple communication protocols
- Ability to handle custom events

• Data Security and Privacy

• Cost of platform

3. OBJECTIVE

Following are the main objectives of our research aimed at analyzing the object capabilities in IoT ecosystem:

- Survey of IoT platforms, along with evaluation and analysis of performance of popular IoT devices with Linux container technologies.
- Security analysis of container technologies and its impact on the performance of one of the popular IoT device obtained above.
- Identification of QoS parameters of devices in IoT environment such as sensor capabilities, memory, energy consumption etc.,
- To analyze and evaluate the effectiveness of an IoT ecosystem based on various object's intelligence capabilities and parameters with deep learning and optimized machine learning techniques.
- Propose the techniques obtained above in order to quickly identify or act on security threats, anomalous activities, etc., that hinders the effectiveness of the IoT ecosystem.

4. ORGANIZATION OF THESIS

Our research on analysis of IoT ecosystem effectiveness based on intelligent object capabilities has been organized as follows:

CHAPTER 1: Introduction

This section gives a detailed insight into the background of IoT system and its architecture, individual components such as connectivity, devices, data processing, user interfaces, future challenges, solutions, container technologies potential application areas of IoT followed by research objectives and contributions has been discussed.

CHAPTER 2: Literature Review

Existing researches and related works with respect to our research in the fields of IoT, Big Data, Cloud Computing, AI, Machine Learning, security aspects, virtualization has been covered extensively.

CHAPTER 3: Comprehensive survey on Internet of Things open source platforms

This chapter encapsulates and summarizes various open source IoT platforms and their characteristics in terms of reliability, scalability, security, interoperability, hardware and software support, which has been evaluated to enrich the researchers and developers with adequate knowledge to locally deploy them according to their requirements before investing on large scale applications.

CHAPTER 4: Analysis of Linux containers in Internet of Things ecosystem using ARM development boards

Performance analysis and evaluation of various ARM developments boards that is available off the shelf to test for the impact of container technology on the performance of CPU, network, memory and I/O devices with the help of benchmarking tools along with bare-metal performance has been discussed, along with the experimental results and analysis.

CHAPTER 5: Secure Internet of Things ecosystem with container virtualization

This section devolves a reference QoS based edge centric computing model incorporating container technologies to ensure security and isolation of services. Host operating system and its required functionalities in resource constrained environments, isolation of services, secure OTA delivery updates has been discussed in detail with results and discussions.

CHAPTER 6: Sensor Cloud Virtualization to improve Internet of Things based WSN

This chapter proposes a novel architecture for the Internet of Medical Devices (IoMD) system to monitor elder people in their homes. In the proposed framework, an intelligent method is introduced to handle massive data collected from the physical layer. The detailed analysis presents that our method could classify the activities with

high accuracy. This study has ensured benefits of the Sensor-Cloud virtualization paradigm for developing innovative applications in different sectors of the IoT system.

CHAPTER 7: Analysis of Internet of Things capabilities using optimized ML and uncertain traffic modelling

This chapter offers an innovative approach for classifying IoT devices is discussed. Our technique is based on calculating the entropy values of various uncertain traffic aspects. Based on uncertain traffic entropy, we describe a novel approach for identifying IoT devices.

CHAPTER 8: Analysis of object capabilities using AI/ML and traffic modelling

To ensure security and enable devices to be more intelligent, AI and Machine learning approaches are adopted to enhance the performance of IoT devices among resource constrained heterogeneous environments. Deep learning based approach like DNN is analyzed for its semi supervised learning methodology for its adoption in IoT Ecosystems to simulate the cognitive tasks of human brain to enhance decision making and propose inferences on trained data-sets.

CHAPTER 9: Conclusion and future enhancements

Research is concluded with concluding section which summarizes all the key features and significant details that restates the research results followed by recommendations for further scope of the research in future.

5. COMPREHENSIVE SURVEY ON INTERNET OF THINGS OPEN SOURCE PLATFORMS

An IoT platform acts as a middle-ware [8] and performs the task of integrating applications with its hardware as well as offer an environment for data processing and analysis. The information from various hardware components are transmitted to applications and the corresponding commands are transferred back to the connected hardware. Every platform offers specific tools and functionalities to implement a particular IoT solution owing to the heterogeneous requirements of users and devices connected to a network. Figure 3, illustrates the various components of an IoT platform.

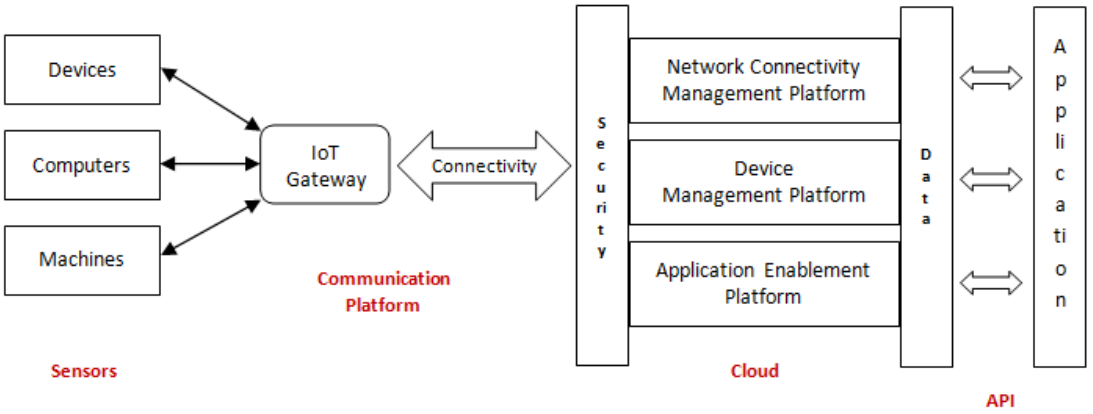

Figure 3: IoT Platform Components

While developing an IoT related application, the utilization of an IoT platform helps the enterprise to focus more on the solution than solving infrastructure related issues and complexities hence improving the business and lowering the time taken for development of applications. There are certain desirable and the essential capabilities of an IoT platform which includes:

- Application development possibilities.
- Ability to manage data with respect to growing network and project complexities.
- Data analytic capabilities such as machine learning, rule engine, processing and visualization.
- Integration and management of multiple devices and inter-operability.
- Secure and efficient data transfer capability.
- Speedy deployment.
- Reduced operational cost.

The need for an out of box deployment of IoT has given rise to a lookout for prospective open source IoT platforms that offers best solutions to meet their requirements in terms of inter-operability among their inter connected heterogeneous devices and robust analytics. Some of the open source IoT platforms taken into account for our survey are as follows:

- Distributed Services Architecture(DSA)
- DeviceHive
- Kaa
- MainFlux

- Thingsboard.io
- SiteWhere
- Zetta
- Node-RED
- Thinger.io
- Thingspeak

In addition to the above said analysis, IoT platforms can be evaluated with respect to their 1) Functionality, 2) Context, 3) Scalability 4) Granularity and 5) Operational Cost.

Since different IoT platforms offer diverse tools to integrate heterogeneous devices, services and applications in an IoT ecosystem[9, 10], the users are required to choose a specific platform that best meets their needs in terms of cost, API, security features, privacy concerns, programming language, device inter-operability, energy consumption etc., to ensure that their system performs as intended.

6. ANALYSIS OF LINUX CONTAINERS IN INTERNET OF THINGS ECOSYSTEM USING ARM DEVELOPMENT BOARDS

System on a chip designers make use of Advanced RISC Machines (ARM) development boards [11] to experiment, evaluate and benchmark the prototypes designed to implement IoT related projects. ARM development boards are available off the shelf to aid the researchers and academia to accelerate the building up of innovative designs and reduce the risks before actual deployment. They are basically printed circuit boards embedded with microprocessors or micro-controllers and support logic to design and evaluate hardware and software designs. They allow easy deployment of various IoT related test cases. Some of the popular ARM boards are

- Raspberry Pi
- DragonBoard 410C
- Pine A64
- Orange Pi PC2
- BeagleBone

Containers offer a standardized, light weight solution to various challenges faced by IoT environment with respect to portability, agility, efficiency, productivity

and security. Modern cloud architecture [12] relies on this phenomenon which bundles the application and all of its associated dependencies in to a single package that can run on any run time environment irrespective of underlying infrastructure. Building, testing and deploying the larger applications using multiple containers is orchestrated in the form of clusters. Another important aspect is the rollback mechanism supported by containers where in the event of any wrong unacceptable update, the containers helps in restoring the device back to previous condition without any disruption.

Some of the popular container technologies [13] are Docker, CRI-O, Linux containers (LXC, LXD), rocktlet, Microsoft containers, kubernetes etc., and Linux containers offer practical and standard development and deployment virtualization technology [13] tool in cloud environments. It offers high resilience to failures, isolated and flexible environment, efficient, portable and more control over the code for the developers.

In our proposed research we have measured the performance of selected ARM development boards as bare metal and with container environment. The objective is to evaluate the effectiveness of the development boards in both the environments and identify if there are any potential drawbacks in utilizing container technology.

Synthetic benchmarks that are used to test the performances of specific sub systems in the hardware under native and with LXC containers are listed below

- Performance of CPU
- Available memory bandwidth
- Network performance between hosts
- Input/ Output performance

The CPU performance results measurements in both the cases (with LXC container and baremetal) matches very closely in Pine A64 and Raspberry Pi boards as illustrated in Figure 4. In case of Dragonboard and Orange Pi, the measurements are close with negligible difference. Time taken for completing the execution is lowest for Dragonboard 410c with 7.50 seconds with baremetal and close 7.49 seconds with LXC container. Longest time for execution has been taken by Raspberry pi model 3 with 15.28 seconds for both baremetal and with LXC container.

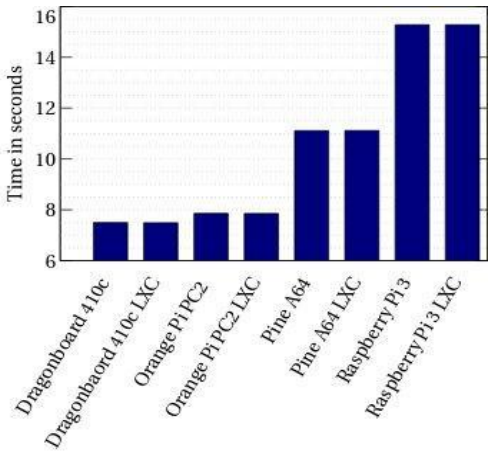

Figure 4: Performance benchmark for CPU

Longest time taken for execution of write operation in memory has been measured for Pine A64 and Dragonboard 410c took least time for execution. Considering the results it is worth noting that compared to other development boards where the container performance did not have significant impact, Pine A64 had large difference of 140.07 seconds inside LXC than 86.80 with baremetal which is shown in Figure 5.

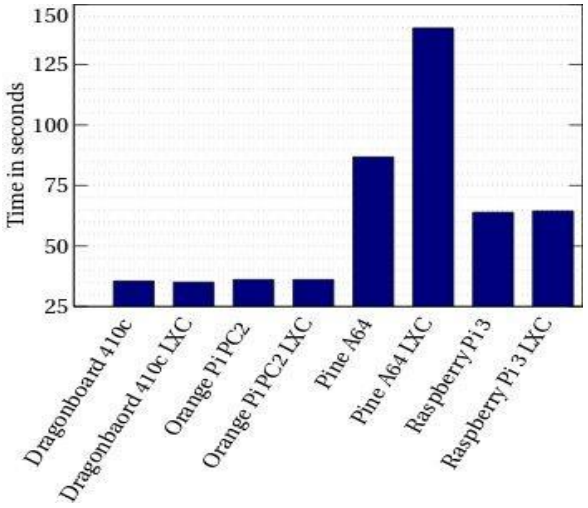

Figure 5: Benchmark for memory performance

In all the above cases, Dragonboard 410c outperformed the rest of the development boards with very minimal deviation from bare-metal to LXC container based benchmarks.

As a system level container LXC promises a light weight solution for conveniently building and controlling the applications in heterogeneous IoT environments. Security and safe delivery has been accomplished with the help of rollback mechanism and frequent software updates. Our contribution is aimed to facilitate developers, researchers and enterprises to choose a development board to meet their needs in accordance with security and operational aspects in IoT Ecosystem.

7. SECURE INTERNET OF THINGS ECOSYSTEM WITH CONTAINER VIRTUALIZATION

As seen in the previous section, container technology offers a perfect solution by offering a light weight solution for inter-operable, portable, distributed heterogeneous environments.

Security updates are critical to protecting the security and privacy of IoT devices in an ecosystem. Updates can be of pull or push type depending upon the type of applications deployed. Traditional deployments mostly prefer pull communication model whereas as far as IoT devices are concerned push model of communication seems to be effective. The reason being less or no human intervention is required to deliver the software and firmware updates in an efficient and up to date manner.

Over The Air updates follows push communication mechanism to deliver the updates in wireless networks. This is accomplished by subscribing to the Original Equipment Manufacturers who in turn will send constant updates at regular intervals. The intervals could be on hourly, weekly or monthly basis depending upon the nature of the fix. In cases of updates sent frequently or small fixes, proper caution must be perused not to disturb the adjoined services or inter-related applications.

Our architecture aims to address the above mentioned scenarios by proposing the following features

- Easy updates without any breakage or interruption
- Safe and secure functioning of IoT devices
- Container technology for service and operating system isolation
- Service overloading

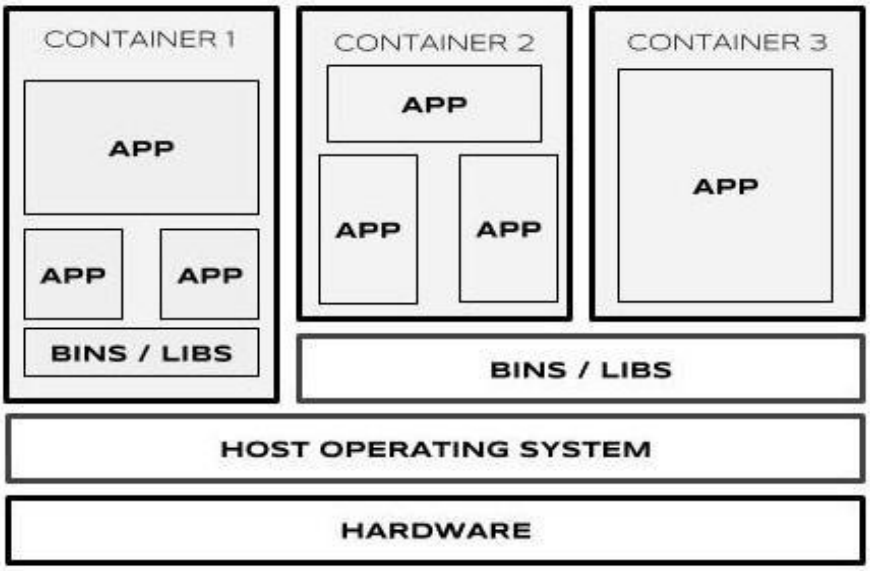

Figure 6: Proposed System Architecture

The design of our proposed system based on edge computing and container virtualization methodology is presented in Figure 6, which has a single kernel and multiple containers in it. Our experiment is based on light weight characteristic feature of con tainer which is proven with the help of Dragonboard 410c development board which encapsulates computational power, Wi-Fi, Bluetooth, and GPS within credit card size module and is widely utilized in edge computing platforms.

The results of the analysis with LXC containers and bare metal without involving the containers are presented in Table 1, below which signifies that both the results for completion time involving the benchmark attributes are more or less similar.

Table 1: Benchmark completion time in seconds

Attributes	**Inside LXC**	**Baremetal**
Memory	35.05	35.01
CPU	7.50	7.50
I/O	9.95	9.70

The principal objective of our research is to take into account the modern containerization technology in facilitating edge computing devices to achieve Quality of Service requirements of heterogeneous devices across the IoT ecosystem. Isolation of services, minimized overhead and security is enhanced by means of our proposed architecture that can even act as a prototype for device vendors, researchers and developers to deliver IoT devices that can function in edge computing environment.

8. SENSOR CLOUD VIRTUALIZATION TO IMPROVE INTERNET OF THINGS BASED WSN

A cloud is a new paradigm for IoT based WSN that overcomes several limitations of traditional WSN and decouples the owners of the physical sensors from the network users. The authors have introduced a Sensor-Cloud and fog virtualization technique and its role in overcoming various limitations of traditional WSN. Figure 7 signifies the proposed Novel Cloud-based IoMD Architecture. There are three key technologies that make up the framework presented: the Internet of Things (IoT), Cloud Computing (CLOUD) and fog Computing (FOG). In our cloud-based architecture, artificial intelligence algorithms are used to process the data collected from IoT enabled medical equipment. We've looked at some of the daily routines of the elderly in order to evaluate the framework we've designed. For this reason, we introduced a neural network [14] method called Deep GAN that runs on the cloud platform and is capable of processing enormous amounts of data quickly and efficiently. UCI Machine Learning Repository data is used to train the proposed Deep GAN for everyday activities recognition.

The experiment is performed using the MATLAB environment with human activity data set from the UCI Repository as described earlier. We have trained our network with various hyper-parameters of GAN model. The structured data set contains certain activities performed by 30 people within the age of 19-48 years. The experiment is carried out by attaching a smart phone (embedded with sensors) on the waist of person and each one performs six different activities. Three are dynamic activities in the data set they are "WALKING, WALKING UPSTAIRS, WALKING DOWNSTAIRS" and three are in the static postures "SITTING, STANDING, LAYING".

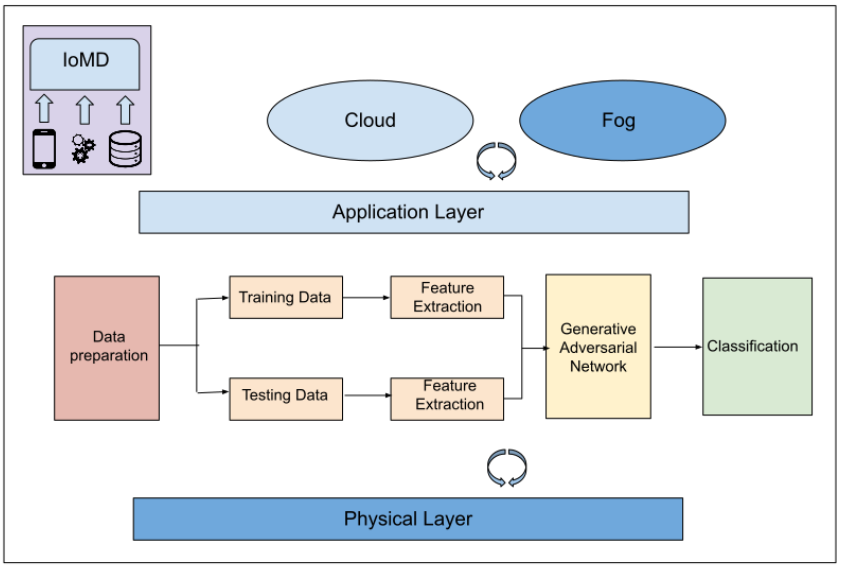

Figure 7: The proposed novel cloud-based IoMD architecture

The accelerometer and gyroscope sensors capture 3-axial angular velocity and 3-axial linear acceleration at a constant rate of 50 Hz and sensor signals were prepossessed by applying noise filters with 0.3 Hz cut-off frequency and the sliding window is 2.56 sec. and the data is labelled manually. The data set is partitioned into 70% for training and 30% for testing.

The comparison of our proposed method with related methods results on the same UCI data set in terms of accuracy is presented in Figure 8. From details analysis and experiment results we found that our proposed Deep GAN method is achieving optimal accuracy of 99.16% in classifying physical activities in comparison to previous methods with respect to UCI HAR data sets.

The detailed analysis presents that our method could classify the activities with high accuracy. Thus, the present case study has ensured benefits of the Sensor-Cloud virtualization paradigm for developing innovative applications in different sectors of the IoT system.

A cloud-aided smart fog gateway for time-sensitive IoT driven healthcare applications was introduced in this section. It ensures that the healthcare applications receive the service at a reasonable delay [15]. Users can expect a quick response from this method. For critical healthcare applications, cloud computing-based IoT architecture is time-sensitive [16]. It's possible to lessen the delay by using the LAN-based Fog Computing Processing method. Additionally, this method helps to limit the amount of data that must be stored on the Cloud. Additionally, Fog

Computing must have memory, processing and compute capabilities, and Fog Nodes can be placed in either LAN or Gateway mode.

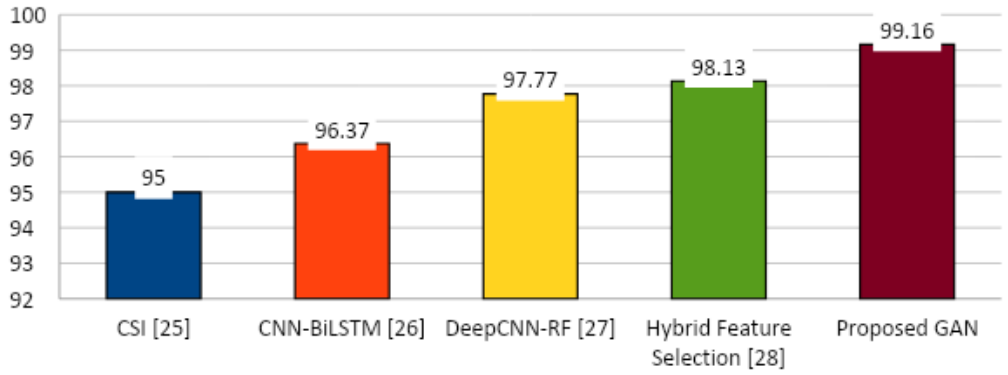

Figure 8: Graphical representation of proposed methods with existing technique

9. ANALYSIS OF IoT CAPABILITIES USING OPTIMIZED ML AND UNCERTAIN TRAFFIC MODELING

The Internet of Things (IoT) incorporates software-based physical devices with sensors which require inter-connectivity to communicate through the internet and be able to exchange data. IoT traffic can be thought of as the aggregate of packets created by various devices in various contexts, such as smart homes or smart cities. These settings contain several sensors, each of which is dedicated to a certain duty, such as monitoring schemes or gathering cyber-physical information. Thus, unlike internet traffic, which has some human-centric features, IoT traffic and sensor devices consistently perform different tasks and make uncertain quantities of data on a regular basis.

In this section the authors propose a method based on calculating the entropy values of various uncertain traffic aspects. The authors describe a novel scheme for identifying IoT devices based on uncertain traffic entropy.

The test-bed consists of five popular Smart Home IoT devices with a Raspberry Pi acting as a gateway. Machine learning (ML) algorithms such as support vector machine (SVM), k-nearest neighbour (KNN) and relevance vector machines (RVM) classifier are used to classify the devices which produce IoT traffic based on uncertain entropy. The learning rate of the classifier model is improved by using the flower pollination optimization (FPO) technique to increase the classifier performance.

The suggested approach minimizes the amount of time spent on optimization operations while maintaining the predictive performance of the induced uncertain models. We work out the entropy standards of traffic characteristics and categorize the uncertain traffic using ML techniques. Our technique successfully identifies devices in a variety of uncertain network situations, with consistent performance in all scenarios. Our technique is also resistant to unpredictability in network behaviour, with abnormalities or uncertainties propagating throughout the network [17].

We have seen before that the entropy values of different traffic features reveal distinct features and can be used to recognize individual gadgets. In this work, we have gathered all uncertain IoT device traffic and recorded it in a single trace. We collected IoT data over several days and have provided findings for one-day traffic because other days exhibit comparable traffic features.

We now want to use ML techniques to sort the devices into different categories. Keeping in mind that the one-day trace we gathered was divided into numerous 5-min ones, we use an Hyper-parameter optimization (HPO) [18] strategy to test our classification's accuracy before applying it to a separate validation data-set. 70% of the total cases (5-min-long tracks) are used in training the model; the remaining 30% are used for validation (30% of the total instances).

Table 2: Performance analysis of the ML classifier without FPO

Methods	Sensitivity	Specificity	F-measure	Accuracy
KNN	75.44	77.36	76.92	77.5
RVM	80.93	80.64	80.95	80.69
SVM	85.24	85	84.19	84.11

Table 2 represents the performance of the proposed classifier without optimization techniques. KNN achieved an accuracy of 77.50%, RVM reached an accuracy of 80.69% and finally, SVM classifier reached better accuracy value of 84.11%. In this comparison, SVM reached maximum accuracy than another given classifier, respectively.

Table 3: Performance analysis of the ML classifier with FPO

Methods	Sensitivity	Specificity	F-measure	Accuracy
KNN	89	87	91.45	96.02
RVM	91	91	93.95	97.07
SVM	93	94	95.19	98.5

Table 3 represent the performance of the proposed classifier with optimization techniques. KNN, with the FPO method achieved an accuracy of 96.02%, RVM reached an accuracy of 97.07% and finally, SVM with the FPO method reached the better accuracy value of 98.50%. In this comparison, SVM with the FPO method reached maximum accuracy than another given classifier, respectively.

10. ANALYSIS OF OBJECT CAPABILITIES USING AI / ML AND TRAFFIC MODELING

Impact of IoT is more on Manufacturing industry which contributes more than 45% to the GDP of growing economy. It's estimated that by 2025 IoT will contribute to more than 40 billion to the economy. CPS (Cyber-Physical-Systems) is a framework that is regulated and supervised by computer algorithms. CPS communicates with networks, physical systems and the virtual arena in an effective way. Integrating IoT with Cyber Physical Systems will result in a hybrid model with superior data exchange facility with more computational power for a manufacturing industry. This hybrid model results in improved network service with stable connectivity and proper access control.

Observing the Traffic pattern on the network ip addresses and ports assists in locating the bottlenecks related to network congestion. Based on the analysis of the bottlenecks and network congestion critical values for the related traffic parameters were calculated.

- IP address of source and the target
- Value of the port used
- Location of port location
- Size of data packet

$$H(X) = -\ n\sum i\ =\ 1p\left(x_i\right)log\left(p\left(x_i\right)\right)$$

x - Refers to the Characteristic that is tested and the value of X ranges from X_1 toX_n

p(x) - Refers to the mass-function related to *x*

Total energy which is not available for consumption (entropy) fluctuates between 0 and log (N). Entropy Value 0 signifies that the data packets are alike and there are no differences in them. Any non-zero value signifies that the data packets have differences, which is calculated as per the above equation. In the upcoming

sections we elaborate about the usage of network patterns to identify the bottlenecks and the traffic congestion on devices.

$$R[A + B + C + \varepsilon < X] = \int_0^{\infty} R_{a+b+c+\varepsilon^{ce^{-xyda}}}$$

$$X = \int_0^{\infty} R_{a+b+c+\vartheta ce^{-xyda}}$$

$$= CR_{a+b+c+\varepsilon(C)}$$

Given the fact that values of a, b, c and ε are not dependent on each other

$$S(t) = R(T < t)$$

Strategy at various nodes are computed using the function R( ) which defines the range. Value of x is binary volatile data exchange model that permits an event to happen. Value of A, B and C variables can be computed using three different methods which use different interoperability calculated means (0, K). Value of complexity is range bound with a lower limit of 0 and higher limit of log (n). This value differs for a different trip limit chosen as defined in the above equations. The value of complexity measured when it is "0" it is in-line with the value computed during examination, though increase in the value of entropy is also seen across different studies. The values computed using these formulas is used across rest of the study to analyze the stress on the device at various network conditions.

Algorithms' performance	**True positive rate (TPR)**	**False positive rate (FPR)**	**Percentage**
SVM	0.6137	0.21452	93%
NN	0.5137	0.21457	91%
NB	0.3996	0.35412	92.01%
DT	0.4137	0.25412	72%
RF	0.2214	0.32515	94.64%
KNN	0.3264	0.21452	92%

Table 4: Comparison of key metrics across ML models

Accuracy of the model using Support Vector and Deep learning algorithms was not up-to the mark during the trial runs. True positive rate of SVM was 0.39 and Deep Learning method was 0.41. Accuracy and TPR of models using Naive Bayes and Decision tree was better when compared to the models discussed earlier. Though the TPR of DN model was better the accuracy was down to 72%. So DN was able to

identify only 72% of the devices correct. All three metrics of Random forest and K-Nearest neighbour was better when compared to other algorithms. Accuracy of RF and KNN were 94% and 92% where as the TPR was 0.2 and 0.3 respectively. Table 4, summarizes the different entropy values and the performance of different algorithms.

11. CONCLUSIONS AND FUTURE WORK

In the first investigation, a detailed analysis of existing open source platforms has been performed to decide upon the suitability of a middle-ware in an application as per the requirement needs of the domain. Parameters considered include the data aggregation, analytics, device management, inter-operability and data processing abilities.

In the second investigation, Linux containers were used to test and evaluate the efficiency of the system by analyzing the effect of container technology on the overall productivity. ARM developments boards were utilized to exactly prototype the targeted domain and benchmark the results obtained using tools such as sysbench to assess and measure its CPU, Memory, disk, I/O performance with LXC containers in comparison with bare metal. Results concluded that containers offered a light weight and portable solution with negligible impact on system performance.

In the third investigation, the objective of edge centric QoS based IoT ecosystem is facilitated by applying container virtualization to isolate the services, enhance the performance by minimizing the overhead and strengthen the security with the help of secured delivery of OTA updates. Researchers, vendors and developers can utilize this prototype to model their designs to give their IoT devices an edge based environment.

In the fourth investigation, a novel architecture for the IoMD system to monitor elder people in their homes. In the proposed framework, an intelligent method is introduced to handle massive data collected from the physical layer. This method called Deep GAN method is running in the cloud layer where rich resources are available on-demand, as well as the reported results, and are made available directly to the application layer through the internet. The detailed analysis presents that our method could classify the activities with high accuracy. This study has ensured benefits of the Sensor-Cloud virtualization paradigm for developing innovative applications in different sectors of the IoT system.

In the fifth investigation, based on uncertain traffic entropy, we describe a novel approach for identifying IoT devices. SVM, KNN and RVM classifiers are used to categorize devices based on the entropy value of uncertain IoT data. To improve the learning rate of the classifier model, we increase the classifier performance by applying the FPO optimization strategy. Our results suggest that we can get a high degree of classification performance, particularly in the situation of intense activity, with 98.50% accuracy. We also train our approach in numerous settings and with uncertain network assaults and it still correctly classifies the IoT devices.

In the sixth investigation, discussion and analysis of existing internet of multimedia things is done to focus on object's capabilities to intelligently predict, monitor the changes in their environments and act accordingly to make strategic decisions. AI and machine learning based DNN approach is utilized to perform cognitive tasks by training the data-sets and optimizes the performance of the system. The authors would also like to address the challenges with respect to device compatibility and longevity to ensure their services don't get disrupted or obsolete when manufacturers no longer offer the service. Opportunities of IoT can be realized only if the required functional aspects and challenges are taken care of along with security and privacy to enable innovation and transformation into a better future.

REFERENCES

[1] Dr. Ovidiu Vermesan, Dr. Peter FriessEU, Internet of Things: Converging Tech nologies for Smart Environments and Integrated Ecosystems, *River Publishers*, (2013).

[2] Martin Serrano, Payam Barnaghi, Francois Carrez Philippe Cousin, Ovidiu Vermesan, Peter Friess, Internet of Things Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps, *IERC*, (2015)

[3] Fengwei Yang, Sai Gu, Industry 4.0, a revolution that requires technology and national strategies, *Complex & Intelligent Systems*, **7** (2021), 1311-1325.

[4] Anichur Rahman, Md. Jahidul Islam, Antonio Montieri, Mostofa Kamal Nasir, Md. Mahfuz Reza, Md. Mahfuz Reza, Shahab S. Band, Antonio Pescape, Mahedi Hasan, Mehdi Sookhak, Amir Mosavi, SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT, *IEEE Access*, **9** (2021), 28361-28376.

[5] Kan Kan Yeung, Ting Huang, Yunzhi Hua, Kai Zhang, Matthew M. F. Yuen, Zhaoli Gao, Recent Advances in Electrochemical Sensors for Wearable Sweat Monitoring: A Review, *IEEE Sensors Journal*, **21** (2021), 14522-14539.

[6] P. Brizzi, D. Conzon, H. Khaleel, R. Tomasi, C. Pastrone, A. M. Spirito, M. Knechtel, F. Pramudianto, P. Cultrona, Bringing the Internet of Things along the Manufacturing Line: A Case Study in Controlling Industrial Robot and Monitoring Energy Consumption Remotely, *IEEE*, (2013).

[7] Leonardo Babun, Kyle Denney, Z. Berkay Celik, Patrick McDaniel, A. Selcuk Uluagac, A survey on IoT platforms: Communication, security, and privacy perspectives, *Computer Networks (Elsevier)*, **192** (2021), 108040.

[8] Davide Conzon, Thomas Bolognesi, Paolo Brizzi, Antonio Lotito, Riccardo Tomasi, and Maurizio A. Spirito. The virtus middleware: An xmpp based architecture for secure iot communications, *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, (2012), 1-6.

[9] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chi-Wei Wang, Chia-Wei Hsu, Chong Kuan Chen, and Shiuh-Pyng Shieh. Iot security: Ongoing challenges and research opportunities, *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, (2014), 230-234.

[10] Sudeendra Kumar, Sauvagya Sahoo, Abhishek Mahapatra, Ayas Kanta Swain, and Kamala Kanta Mahapatra. Security enhancements to system on chip devices for

IoT perception layer, *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, Bhopal, India, (2017), 151-156.

[11] C. P. Kruger and G. P. Hancke. Benchmarking internet of things devices, *2014 12th IEEE International Conference on Industrial Informatics (INDIN)*, (2014), 611-616.

[12] Mussab Alaa, A.A. Zaidan, B.B. Zaidan, Mohammed Talal, and M.L.M. Kiah. A review of smart home applications based on internet of things, *Journal of Network and Computer Applications*, **97** (2017), 48-65.

[13] Harold Kilpatrick. 5 infamous iot hacks and vulnerabilities. In Available online: *https://www.iotsworldcongress.com/5-infamous-iot-hacks-and-vulnerabilities/*, (2020).

[14] R. Du, S. MagnÃºsson, and C. Fischione, The Internet of Things as a Deep Neural Network, *https:// arxiv.org/ abs/2003.10538*, (2020), accessed Mar. 25, 2020.

[15] Y. Hu et al., Learning Privately Over Distributed Features: An ADMM Sharing Approach, *https:// arxiv.org/ abs/1907.07735*, (2019), accessed Dec. 1, 2019.

[16] D. Zayas and P. Merino, The 3GPP NB-IoT System Architecture for the Internet of Things, *Proc. IEEE ICC Wksps.*, (2017), 277-282.

[17] H. Nguyen-An, T. Silverston, T. Yamazaki, T. Miyoshi, Generating IoT traffic: A Case Study on Anomaly Detection, *Proceedings of the IEEE International Symposium on Local and Metropolitan Area Networks*, (2020), 1-6.

[18] K. Muhammad et al., Cost-Effective Video Summarization Using Deep Cnn With Hierarchical Weighted Fusion for Iot Surveillance Networks, *IEEE Internet of Things Journal*, **7** (5) (2020), 4455-4463.

LIST OF PUBLICATIONS

1) S. Senthil Kumaran, S. P. Balakannan and J. Li, A deep analysis of object capabilities for intelligence considering wireless IoT devices with the DNN approach. *The Journal of Supercomputing*, **78** (4) (2022), 4745-4758

2) S. Senthil Kumaran and S. P. Balakannan, Securing Internet of Things Devices Using Containers, *Sustainable development in engineering and technology*, (2022), 137-148

3) S. Senthil Kumaran and S. P. Balakannan, IoT Capabilities Analysis by using Optimized Machine Learning with Uncertain Traffic Modeling, *Journal of Uncertain Systems*, (2023), 2242005

4) S. Senthil Kumaran and S. P. Balakannan, Sensor cloud virtualisation systems for improving performance of IoT-based WSN, *International Journal of Wireless and Mobile Computing*, **24** (1) (2023), 38-47

5) S. Senthil Kumaran and S. P. Balakannan, A Performance Evaluaion of Linux Containers on Similar Arm Based Internet of Things Development Boards, *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, (2018), 1019-1024